GeekBrains

Урок 7 Тема 1

Введение в антиотладочные приемы

Реверс-инжиниринг

В этом видео

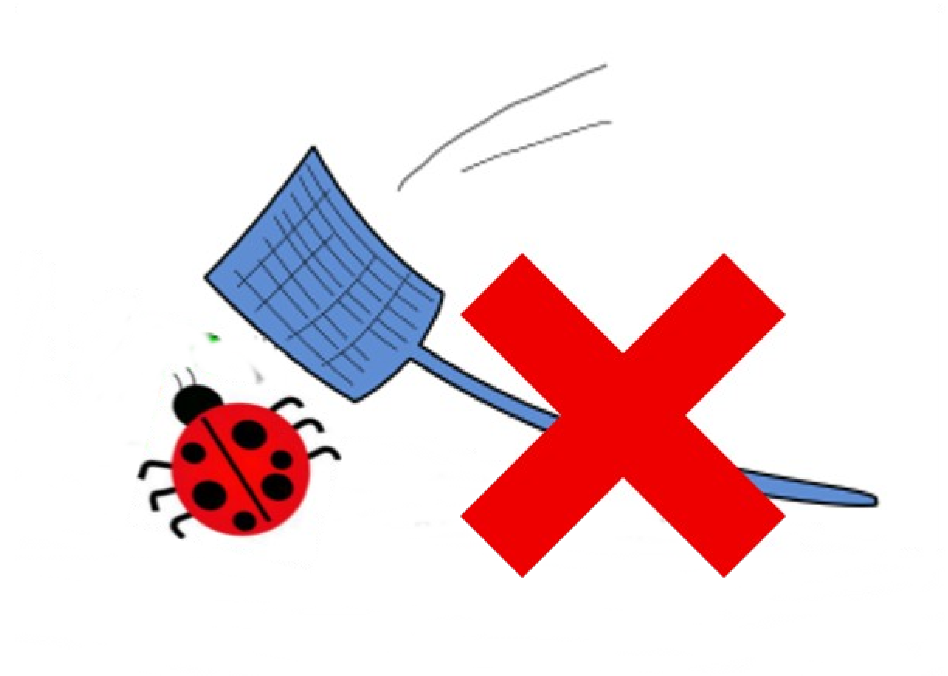
1. Общая информация.
2. Защита от статического анализа.
3. Защита от динамического анализа.

GeekBrains

Общая информация

Где можно встретить антиотладочные приемы?

- Вредоносное ПО (малварь).
- Проприетарное ПО.



Защита от статического анализа

Способы защиты от статического анализа:

- Обфускация кода:
  - перед компиляцией;
  - в процессе компиляции;
- Применение упаковщиков (пакеров):
  - UPX;
  - ASPack.

GeekBrains

Обфускация кода перед компиляцией

Было:

```
...
int packetLength = 255;
char *getPacket(char *);
...
```

Стало:

```
...
int asdkajr1dfa = 255;
char *asdfljakbw23fad(char *);
...
```

Обфускация кода в процессе компиляции

Оптимизация кода средствами компилятора:

- Оптимизация по размеру:
  - gcc: -Os
  - cl (msvc): /O1
- Оптимизация по скорости:
  - gcc: -O3
  - cl (msvc): /O2

Применение упаковщиков (пакеров)

Процесс упаковки программы

Бинарный файл
+
Упаковщик
=>
Упакованный бинарный файл
+
Распаковщик

Процесс запуска программы

Упакованный бинарный файл
+
Распаковщик
=>
Передача управления на распакованный код программы

GeekBrains

Защита от динамического анализа

Способы защиты от динамического анализа:

- обнаружение виртуального окружения;
- обнаружение отладчика.

Итоги

1. Получили общую информацию по антиотладочным приемам.
2. Узнали, как антиотладочные приемы защищают программы от статического и динамического анализа.

GeekBrains